REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Priority Claim

The Applicant respectfully traverses the Examiner's allegation that the priority claim for the present application, on the grounds that the end of the one-year period specified in 35 USC §119 (January 25, 2000) fell on a Saturday, and the present application was submitted on the following Monday, January 27, 2000.

Claiming priority based on a Monday filing of an application whose one-year term ended on a Saturday is permitted by 35 USC §21 and Article 4C(3) of the Paris Convention, which provides:

> *. . .if the last day on which the Office is not open for the filing of applications in the country where protection is claimed, the period shall be extended until the first following working day.*

See also, MPEP 201.13 E. (Page 200-82), which provides:

> *. . .if the 12 months expires on a Saturday, the U.S. application may be filed on the following Monday."*

Withdrawal of the indication that a claim for priority cannot be based on the application filed in Germany on January 25, 1999, is therefore respectfully requested.

2. Rejection of Claims 2 and 8 Under 35 USC §112, 2nd Paragraph

This rejection has been addressed by deleting the objected-to "in particular" language in original claims 2 and 8 (and corresponding language in claim 3).

Withdrawal of the rejection under 35 USC §112, 2nd Paragraph is therefore respectfully requested.

3. Rejection of Claims 1 and 3-8 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman) and 6,038,551 (Barlow)

This rejection is respectfully traversed on the grounds that neither the Hellman patent nor the Barlow patent, whether considered individually or in any reasonable combination, discloses or suggests a chipcard initialization step in which:

- parts of respective first and second "values" generated by the card *and* processing station;
- the processing station generates a secret initial value from at least part of the first value and the transmitted part of the second value; and
- the chip card generates the secret initial value from at least part of the second value and the transmitted part of the first value.

The purpose of the claimed invention is to provide a method of initializing a chipcard by providing the chipcard and processing station with secret values that can be used as the basis for transferring secret keys that can be used in further information exchanges by the chipcard and processing station, without actually exchanging the secret values. The method only transmits parts of values used to calculate the secret values, thereby protecting the secret values from interception.

In the system of Hellman, the "conversers" already "*each possess a secret signal and exchange an initial transformation of the secret signal with the other converser*" (see, *e.g.*, the abstract of Hellman). While the secret signals of Hellman correspond to the secret values of the claimed invention in the sense that they can be used to facilitate further encrypted communications, and in particular the generation of shared secret keys, these secret signals must themselves be exchanged in order to enable subsequent key exchanges. Unlike the claimed invention, which only transmits parts of respective first and second values, Hellman takes the approach of protecting the "secret signals" by "transforming" the secret signals before their exchange. While such exchanges can be made relatively secure through the use of one-way function transformations, the protection is not perfect. In contrast, the claimed invention does

require any exchange of the secret values, whether transformed or not. Instead, only parts of the values are exchanged.

The Barlow patent, on the other hand, teaches a system that not only exchanges secret keys, but does so by means of public key encryption of the exchanged secret keys. Barlow makes no attempt to only exchange parts of secret values, but rather simply encrypts all of the values before exchange (col. 3, lines 1-13). This public key method of Barlow is not suitable for chipcard initialization of the type claimed, and Barlow does not even remotely suggest a method of generating an initialization value without exchanging the values.

According to the claimed invention, initial values can be generated for each chipcard manufactured in a relatively simple and yet secure manner. Barlow, on the other hand, points out the difficulty of providing millions of different devices with individual keys. This is hardly suggestive of a method that might be applied to chipcard initialization, or of a method that could be combined with the secret value generation and exchange of Hellman to obtain the claimed invention. As a result, it is respectfully submitted that no combination of the Hellman and Barlow patents could possibly have suggested the claimed invention to the ordinary artisan, and withdrawal of the rejection of claims 1 and 3-8 under 35 USC §103(a) is respectfully requested.

4. Rejection of Claim 2 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman) and 6,038,551 (Barlow), and "*Cryptographic Identification Methods For Smart Cards In the Process of Standardization*" (Konigs)

This rejection is respectfully traversed on the grounds that the Konigs article, like the Hellman and Barlow patents, fails to disclose or suggest a chipcard initialization method in which secret values are established for the chipcard and processor to use in subsequent communications, such as for use in transferring a secret key to the card, *without an exchange of the "secret values,"* by exchanging only parts of the secret values generated by the chipcard and processor.

Instead, the Konigs article, again like the Hellman and Barlow patents, discloses a method of establishing cryptographic data connections using chipcards without containing any suggestion as to how the chipcards used for the cryptographic data connections are initialized for use in the cryptographic connections. As a result, withdrawal of the rejection of claim 2 under 35 USC §103(a) is respectfully requested.

5. Rejection of Claim 9 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman), 6,038,551 (Barlow), and 5,224,163 (Gasser)

This rejection is respectfully traversed on the grounds that the Gasser patent, like the Hellman patent and the Barlow patent, fails to disclose a card initialization step in which transfer of data to the card is facilitated by a "secret value" exchange that only involves transfer of "parts" of the respective secret values, and that does not require transformation of the secret values.

Instead, the Gasser patent disclose generation of "session public/private encryption key pairs." The session public/private key pairs are generated, as is common in such session key generating schemes, by mutual exchange and processing of secret values, but there is no disclosure in the Gasser patent that the secret values used in the public/private session key generating process may be transferred to the chipcard by a secret value generated in the manner claimed, using parts of two picnics in the manner claimed. According, withdrawal of the rejection of claim 9 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: December 29, 2003

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500